REMARKS

Claims 82-116 remain in this application. In view of the following remarks, Applicant requests favorable considerable and timely indication of allowance.

Claims 82-84, 86, 88-90, 92-94, 96, 97, 103, 104 and 106-116 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg (U.S. 6,240,091) in view of a publication entitled *Applied Cryptography* 2nd Edition, October 1995, by Schneier. Claim 85 has been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claim 82, and further in view of Walker (U.S. 6,263,438). Claims 87, 91, 95, 98-102, and 105 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claim 84, and further in view of facts in which the Patent Office has taken official notice. These rejections are respectfully traversed.

Applicant discloses a novel and unobvious cryptographic system for secure communications between a member and a service provider. Applicant's cryptographic system provides an improvement over conventional approaches by providing security without the need for a secret key or a trusted third party. In one embodiment of the cryptographic system, the member initiates communications with a service provider by sending a key exchange request message. The key exchange request message includes the member's public key, and encrypted, at least in part, with the service provider's public key stored on an electronic or smart card of the member. The service provider, in response to the key exchange request message, generates a session key to be used to conduct a transaction between the two.

The Patent Office relies on Ginzboorg for disclosing an electronic card with the public key of a service provider, but admittedly does not disclose any other feature of Applicant's approach. According to the Patent Office, these features are disclosed by Schneier's Woo-Lam protocol. In particular, the Patent Office contends that a member using the Woo-Lam protocol generates a key exchange request message that includes the member's public key, and encrypts the at least a portion of the message with the service provider's public key. The Patent Office further contends that the service provider, in response to the key exchange request, generates a session key and sends it to the member to conduct the transaction. The Patent Office relies on an

Encrypted Key Exchange protocol disclosed in Schneier for a key exchange protocol where one participant is exclusively tasked with generating the session key.

The position taken by the Patent Office fails for at least two reasons. First, there is no teaching or suggestion in the prior art to support the combination of references. Second, even if one were to attempt to combine these references, as proposed by the Patent Office, the resultant combination would still not yield the claimed invention.

A. *The Prior Art Does Not Suggest the Desirability of the Claimed Invention.*

According to the Patent Office, the "desire to verify digital signature" in Ginzboorg provides the motivation for combining Ginzboorg with the Woo-Lam protocol. Applicant respectfully disagrees. Ginzboorg's system discloses the use of a subscriber database at the service provider site that contains the public keys from all the subscribers. For example, in column 8, lines 66-67 and column 9, lines 1-3, Ginzboorg states that "[a]fter having received the signed contract CDR, the charging server WD verifies the signature by using known method in order to authenticate the CDR. For this purpose, the charging server receives from its subscriber database the public for the customer in question (arrow C in Fig 5)." It is clear that Ginzboorg already has the ability to verify digital signatures from its subscribers and therefore has no reason to work with Woo-Lam or the EKE protocols for this purpose.

In addition, there is no motivation to combine the Otway-Rees protocol with Ginzboorg and/or the Woo-Lam protocol. Otway-Rees is a secret key based protocol. Every member in the protocol must share a pre-arranged secret key with the service provider in order for the protocol to work. The protocol discloses a method for the trusted server Trent to provide a symmetric key to two members of the network, Alice and Bob. Since neither Ginzboorg nor Woo-Lam uses any pre-arranged shared secret, it is improper to combine them with Otway-Rees as suggested by the Patent Office.

B. *The Prior Art Does Not Teach or Suggest All the Claim Limitations.*

The Patent Office acknowledges that neither Ginzboorg nor Schneier discloses the transmission of the member's public key to the service provider. Instead, the Patent Office relies on Walker for this feature. However, Walker does not disclose the process of sending of a keyThe combination of references proposed by the Patent Office does not establish a *prima facie* case of obviousness. First, contrary to the position taken by the Patent Office, the key exchange

request generated by a member using the Woo-Lam protocol does not include the member's public key. Referring to step 3 of the Woo-Lam protocol, the key exchange request generated by the member (Alice) includes only the service provider's name (Bob) and a random number, the combination being encrypted with the service provider's public key. The service provider receives the member's public key not from the member, but rather from a trusted third party (Trent). (See Woo-Lam protocol, step 5).

Second, it is improper for the Patent Office to rely on the Encrypted Key Exchange protocol for the concept of generating a session key exclusively at the service provider. In Schneier's Encrypted Key Exchange Protocol, the session key is generated by one of the participants using a shared secret or symmetric key P. Referring to step 2 of the Encrypted Key Exchange protocol, the session key is generated by Bob and encrypted with Alice's public key and the secret key P. In other words, Schneier's Encrypted Key Exchange protocol teaches that a session key may generated by one of the participants only if they share a secret key. Since neither Ginzboorg nor the Woo-Lam protocol use a secret key, it would be improper to modify the combination of Ginzboorg and Woo-Lam in the manner suggested by the Patent Office based on the teachings of Schneier's Encrypted Key Exchange protocol.

Consider now the independent claims. Claims 82, 96, 103, 109 and 113 each recite sending a key exchange request message from a member to a service provider, the key exchange request message having the public key of the member. Claims 82, 96, 103, 109 and 113 further recite generating a session key exclusively at the service provider in response to the key exchange message request. As discussed above, the Woo-Lam protocol of Schneier does not call for sending the member's public key to the service provider in the key exchange request message. Instead, the member's public key is received by the service provider from a trusted third party. Moreover, Schneier's Encrypted Key Exchange protocol does not teach or suggest that a service provider, which does not share a secret key with a member, should generate the session key. Accordingly, the combination of Ginzboorg and Schneier is legally insufficient to establish a *prima facie* case of obviousness.

Claims 83-95, 97-102, 104-108, 110-112, and 114-116 are either dependent from claim 82, 96, 103, 109 or 113, and therefore, incorporate all the limitations of the claim from which they respectively depend. Accordingly, these claims are also allowable for the same reasons set forth hereinbefore, as well as the additional limitations cited therein. These additional

limitations will not be addressed at this time because the Patent Office has not established a *prima facie* case of obviousness against the independent claims.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested. Should any issues remain which the Examiner believes could be resolved in a telephone interview, the Examiner is requested to telephone Applicant's undersigned attorney.

Respectfully submitted,

4-18-05
Date

Craig A. Gelfound
Registration No. 41,032

McDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
Telephone: (310) 277-4110
Facsimile: (310) 277-4730